EXAMPLES OF MORDELL'S EQUATION

KEITH CONRAD

1. Introduction

The equation $y^2 = x^3 + k$, for $k \in \mathbf{Z}$, is called Mordell's equation[1] due to Mordell's work on it throughout his life. A natural number-theoretic task is describing all of its solutions in $\mathbf{Z}$ or $\mathbf{Q}$, either qualitatively (decide if there are finitely or infinitely many solutions in $\mathbf{Z}$ or $\mathbf{Q}$) or quantitatively (list or otherwise conveniently describe all such solutions). In 1920, Mordell [10] showed that for each nonzero $k \in \mathbf{Z}$, $y^2 = x^3 + k$ has finitely many integral solutions. Rational solutions are a different story: there may be finitely or infinitely many, depending on k. Whether there are finitely or infinitely many rational solutions is connected to a central topic in number theory: the rank of an elliptic curve.

Here we will describe all integral solutions to Mordell's equation for some selected values of k,[2] and make a few comments at the end about rational solutions. For further examples of the techniques we use to find integral solutions, see [1, Chap. 14].

2. Examples without Solutions

To prove $y^2 = x^3 + k$ has no integral solution for specific values of k, we will use congruence and quadratic residue considerations. Specifically, we will use the following descriptions of when -1, 2, and -2 are squares modulo odd primes p, writing "$\square$" to mean a square:

$$\begin{aligned} -1 \equiv \square \bmod p &\iff p \equiv 1 \bmod 4, \\ 2 \equiv \square \bmod p &\iff p \equiv 1, 7 \bmod 8, \\ -2 \equiv \square \bmod p &\iff p \equiv 1, 3 \bmod 8. \end{aligned}$$

Our first three theorems will use the criterion for $-1 \equiv \square \bmod p$.

Theorem 2.1. *The equation $y^2 = x^3 + 7$ has no integral solutions.*

Proof. Assume there is an integral solution (x, y). If x is even then $y^2 \equiv 7 \bmod 8$, but 7 mod 8 is not a square. Therefore x is odd. Rewrite $y^2 = x^3 + 7$ as $y^2 + 1 = x^3 + 8$, so

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4). \tag{1}$$

Note $x^2 - 2x + 4 = (x - 1)^2 + 3$ is at least 3. Since x is odd, $(x - 1)^2 + 3 \equiv 3 \bmod 4$. Thus $x^2 - 2x + 4$ has a prime factor $p \equiv 3 \bmod 4$: if not, all of its prime factors are 1 mod 4, so $x^2 - 2x + 4 \equiv 1 \bmod 4$ since a *positive* integer is the product of its prime factors (this isn't true for -5: $-5 \equiv 3 \bmod 4$ and the prime factor of -5 is 1 mod 4). That contradicts $x^2 - 2x + 4 \equiv 3 \bmod 4$. From $p \mid (x^2 - 2x + 4)$ we get $p \mid (y^2 + 1)$ by (1), so $y^2 + 1 \equiv 0 \bmod p$. Thus $-1 \equiv \square \bmod p$, contradicting $p \equiv 3 \bmod 4$. This is V. A. Lebesgue's method [8].

[1] Also called Bachet's equation.

[2] Large tables of k and their integral solutions are at https://hr.userweb.mwn.de/numb/mordell.html and https://secure.math.ubc.ca/~bennett/BeGa-data.html.

Here's another approach, using the factor $x+2$ instead of the factor x^2-2x+4. Since (as seen above) x is odd and y is even, $x^3 \equiv x \bmod 4$ (true for all odd x), so reducing $y^2 = x^3+7$ modulo 4 gives us $0 \equiv x+3 \bmod 4$, so $x \equiv 1 \bmod 4$. Then $x+2 \equiv 3 \bmod 4$. Moreover, $x+2 > 0$, since if $x \leq -2$ then $x^3 \leq -8$, so $x^3+7 \leq -1$, which contradicts x^3+7 being a perfect square. From $x+2$ being positive and congruent to 3 mod 4, it has a prime factor $p \equiv 3 \bmod 4$, so $y^2+1 \equiv 0 \bmod p$ from (1) and we get a contradiction as before. □

Theorem 2.2. *The equation $y^2 = x^3 - 5$ has no integral solutions.*

Proof. Assuming there is a solution, reduce modulo 4:

$$y^2 \equiv x^3 - 1 \bmod 4.$$

Here is a table of values of y^2 and x^3-1 modulo 4:

y	$y^2 \bmod 4$	x	$x^3-1 \bmod 4$
0	0	0	3
1	1	1	0
2	0	2	3
3	1	3	2

The only common value of $y^2 \bmod 4$ and $x^3-1 \bmod 4$ is 0, so y is even and $x \equiv 1 \bmod 4$. Then rewrite $y^2 = x^3 - 5$ as

$$y^2 + 4 = x^3 - 1 = (x-1)(x^2+x+1). \tag{2}$$

Since $x \equiv 1 \bmod 4$, $x^2+x+1 \equiv 3 \bmod 4$, so x^2+x+1 is odd. Moreover, $x^2+x+1 = (x+1/2)^2 + 3/4 > 0$, so $x^2+x+1 \geq 3$. Therefore x^2+x+1 must have a prime factor $p \equiv 3 \bmod 4$ (same reasoning as in the previous proof). Since p is a factor of x^2+x+1, p divides y^2+4 by (2), so $y^2+4 \equiv 0 \bmod p$. Therefore $-4 \equiv \square \bmod p$, so $-1 \equiv \square \bmod p$. This implies $p \equiv 1 \bmod 4$, contradicting $p \equiv 3 \bmod 4$. □

Theorem 2.3. *The equation $y^2 = x^3 + 11$ has no integral solutions.*

Proof. We will use ideas from the proofs of Theorems 2.1 and 2.2.

Assume there is an integral solution (x, y). Since $11 \equiv -1 \bmod 4$, the same reasoning as in the proof of Theorem 2.2 shows $x \equiv 1 \bmod 4$.

Rewrite $y^2 = x^3 + 11$ as

$$y^2 + 16 = x^3 + 27 = (x+3)(x^2-3x+9). \tag{3}$$

The factor x^2-3x+9 is positive (why?), and from $x \equiv 1 \bmod 4$ we get $x^2-3x+9 \equiv 3 \bmod 4$, so by the same reasoning as in the proof of Theorem 2.1, x^2-3x+9 has a prime factor p with $p \equiv 3 \bmod 4$. Therefore $p \mid (y^2+16)$ by (3), so $-16 \equiv \square \bmod p$. Since p is odd, $-1 \equiv \square \bmod p$, and that contradicts $p \equiv 3 \bmod 4$. □

Our next two theorems will rely on the condition for when $2 \equiv \square \bmod p$.

Theorem 2.4. *The equation $y^2 = x^3 - 6$ has no integral solutions.*

Proof. Assume there is an integral solution. If x is even then $y^2 \equiv -6 \equiv 2 \bmod 8$, but 2 mod 8 is not a square. Therefore x is odd, so y is odd and $x^3 = y^2+6 \equiv 7 \bmod 8$. Also $x^3 \equiv x \bmod 8$ (true for all odd x), so $x \equiv 7 \bmod 8$.

Rewrite $y^2 = x^3 - 6$ as

$$y^2 - 2 = x^3 - 8 = (x-2)(x^2+2x+4), \tag{4}$$

with $x^2+2x+4 \equiv 7^2+2\cdot 7+4 \equiv 3 \bmod 8$. Since $x^2+2x+4=(x+1)^2+3$ is positive, it must have a prime factor $p \equiv \pm 3 \bmod 8$ because if all of its prime factors are $\pm 1 \bmod 8$ then $x^2+2x+4 \equiv \pm 1 \bmod 8$, which is not true. Let p be a prime factor of x^2+2x+4 with $p \equiv \pm 3 \bmod 8$. Since p divides y^2-2 by (4), we get $y^2 \equiv 2 \bmod p$. Thus $2 \equiv \square \bmod p$, so $p \equiv \pm 1 \bmod 8$, which is a contradiction.

We can get a contradiction using the factor $x-2$ also. Since $x \equiv 7 \bmod 8$, $x-2 \equiv 5 \bmod 8$. Also $x-2>0$, since if $x \leq 2$ and $x-2 \equiv 5 \bmod 8$ then $x \leq -1$, but then x^3-6 is negative so it can't be a perfect square. From $x-2$ being positive and congruent to 5 mod 8, it has a prime factor $p \equiv \pm 3 \bmod 8$ and then $y^2 \equiv 2 \bmod p$ and we get a contradiction in the same way as before. □

Theorem 2.5. *The equation $y^2=x^3+45$ has no integral solutions.*

Proof. Assume there is an integral solution. If y is odd then $x^3=y^2-45 \equiv 1-45 \equiv 4 \bmod 8$, which is impossible. Therefore y is even, so x is odd. Reducing the equation mod 4, $0 \equiv x^3+1 \bmod 4$. Since $x^3 \equiv x \bmod 4$ for odd x, $x \equiv 3 \bmod 4$. Also, y is not a multiple of 3. If $3 \mid y$ then the equation $y^2=x^3+45$ shows 3 divides x. Write $x=3x'$ and $y=3y'$, so $9y'^2=27x'^3+45$, so $y'^2=3x'^3+5$, which implies $y'^2 \equiv 2 \bmod 3$, and that is impossible.

We will now take cases depending on whether $x \equiv 3 \bmod 8$ or $x \equiv 7 \bmod 8$. (If you know an elementary method that treats both cases in a uniform way, please tell me!)

Case 1: $x \equiv 3 \bmod 8$. Rewrite $y^2=x^3+45$ as

$$y^2-72=x^3-27=(x-3)(x^2+3x+9). \tag{5}$$

The factor $x^2+3x+9=(x+3/2)^2+27/4$ is positive and is congruent to 3 mod 8, so it has a prime factor $p \equiv \pm 3 \bmod 8$. Feeding this into (5),

$$y^2 \equiv 72 \equiv 2\cdot 6^2 \bmod p. \tag{6}$$

We can't have $p=3$ (just in case $p \equiv 3 \bmod 8$, this is something we need to deal with) since it would imply $y^2 \equiv 0 \bmod 3$, but we already checked y is not a multiple of 3. Since p is not 3, (6) implies $2 \equiv \square \bmod p$, so $p \equiv \pm 1 \bmod 8$, contradicting $p \equiv \pm 3 \bmod 8$.

Case 2: $x \equiv 7 \bmod 8$. Rewrite $y^2=x^3+45$ as

$$y^2-18=x^3+27=(x+3)(x^2-3x+9). \tag{7}$$

The factor $x^2-3x+9=(x-3/2)^2+27/4$ is positive and is congruent to 5 mod 8, so it has a prime factor $p \equiv \pm 3 \bmod 8$. From (7) we get $y^2 \equiv 18 \equiv 2\cdot 3^2 \bmod p$. Arguing as in Case 1, we again find $p \equiv \pm 1 \bmod 8$, which is a contradiction. □

In our next two theorems we will use the condition for when $-2 \equiv \square \bmod p$.

Theorem 2.6. *The equation $y^2=x^3+6$ has no integral solutions.*

Proof. Mordell [11, p. 22-23], [12, p. 70] proved this using $\mathbf{Z}[\sqrt{6}]$. The simpler method used here, which resembles the proof of Theorem 2.4, is due to Shiv Gupta and Tracy Driehaus.

Assume there is an integral solution. First we will show x is odd, and in fact $x \equiv 3 \bmod 8$. If x is even then $y^2 \equiv 6 \bmod 8$, which is impossible. Thus x is odd, so y is odd and $x^3=y^2-6 \equiv -5 \equiv 3 \bmod 8$. Since $x^3 \equiv x \bmod 8$, we have $x \equiv 3 \bmod 8$.

Rewrite $y^2=x^3+6$ as

$$y^2+2=x^3+8=(x+2)(x^2-2x+4), \tag{8}$$

with $x^2-2x+4 \equiv 3^2-2\cdot 3+4 \equiv 7 \bmod 8$. For each prime factor p of x^2-2x+4, $y^2+2 \equiv 0 \bmod p$, so $-2 \equiv \square \bmod p$, and therefore $p \equiv 1, 3 \bmod 8$. Then since $x^2-2x+4=$

$(x-1)^2+3$ is positive, x^2-2x+4 is 1 or 3 mod 8. We showed before that this number is 7 mod 8, so we have a contradiction.

To get a contradiction using the factor $x+2$, first note that this number is positive, since if $x+2<0$ then $y^2+2\leq 0$, which is impossible. For a prime p dividing $x+2$, $y^2+2\equiv 0 \bmod p$, so $p\equiv 1$ or 3 mod 8. Therefore $x+2\equiv 1$ or 3 mod 8. However, since $x\equiv 3 \bmod 8$ we have $x+2\equiv 5 \bmod 8$, which is a contradiction. □

Theorem 2.7. *The equation $y^2=x^3+46$ has no integral solutions.*

Proof. Assume there is an integral solution. If x is even then $y^2\equiv 6 \bmod 8$, which has no solution, so x is odd and y is odd. Thus $y^2\equiv 1 \bmod 8$ and $x^3\equiv x \bmod 8$, so $1\equiv x+6 \bmod 8$, making $x\equiv 3 \bmod 8$.

Now rewrite $y^2=x^3+46$ as

$$y^2+18=x^3+64=(x+4)(x^2-4x+16). \tag{9}$$

Since $x\equiv 3 \bmod 8$, the first factor on the right side of (9) is 7 mod 8 and the second factor is 5 mod 8. We will get a contradiction using either of these factors.

First we work with the quadratic factor $x^2-4x+16=(x-2)^2+12$, which is positive. Since it is 5 mod 8, it must have a prime factor p that is not 1 or 3 mod 8. Indeed, if all the prime factors of $x^2-4x+16$ are 1 or 3 mod 8 then so is $x^2-4x+16$, since $\{1,3 \bmod 8\}$ is closed under multiplication. But $x^2-4x+16\not\equiv 1,3 \bmod 8$. The prime p, not being 3 mod 8, is in particular not equal to 3. Also, $p\neq 2$ since $x^2-4x+16$ is odd. Since $p\mid (x^2-4x+16)$ we get by (9) that $p\mid (y^2+18)$, so $y^2\equiv -18 \bmod p$. Hence $-18\equiv \square \bmod p$, so $-2\equiv \square \bmod p$. This implies $p\equiv 1$ or 3 mod 8. But $p\not\equiv 1$ or 3 mod 8, so we have a contradiction.

To get a contradiction using the factor $x+4$, first let's check it is positive. There is no solution to $y^2=x^3+46$ when y^2 is a perfect square less than 46 (just try $y^2=0,1,4,9,16,25,36$; there is no corresponding integral x), which means we must have $x^3>0$, so $x>0$. Thus $x+4>1$. Since $x+4\equiv 7 \bmod 8$, $x+4$ must have a prime factor p that is not 1 or 3 mod 8, just as before. The prime p is not 2 since $x+4$ is odd, and $p\neq 3$ since $p\not\equiv 3 \bmod 8$. Then $y^2\equiv -18 \bmod p$ from (9) and we get a contradiction as before. □

Our next theorems uses the conditions for $-1 \bmod p$ and $-2 \bmod p$ to be squares.

Theorem 2.8. *The equation $y^2=x^3-24$ has no integral solutions.*

Proof. We take our argument from [13, pp. 271–272], which is based on [14, p. 201].

Assuming there is an integral solution (x,y), we show x is even. Rewrite $y^2=x^3-24$ as

$$y^2+16=x^3-8=(x-2)(x^2+2x+4).$$

The factor x^2+2x+4 equals $(x+1)^2+3$, which is at least 3. If x is odd then $(x+1)^2+3\equiv 3 \bmod 4$, so $(x+1)^2+3$ has a prime factor p such that $p\equiv 3 \bmod 4$. Then $y^2\equiv -16 \bmod p$, so $-1\equiv \square \bmod p$. This contradicts the condition $p\equiv 3 \bmod 4$. Therefore x is even, so also y is even.

From $y^2=x^3-24$ we get $8\mid y^2$, so $4\mid y$. Write $x=2x'$ and $y=4y'$. Then $16y'^2=8x'^3-24$, which implies $2y'^2=x'^3-3$, so x' is odd and greater than 1. Rewrite $2y'^2=x'^3-3$ as

$$2(y'^2+2)=x'^3+1=(x'+1)(x'^2-x'+1).$$

The factor $x'^2-x'+1$ is odd and greater than 1. Let p be a prime factor of it, so $y'^2\equiv -2 \bmod p$, which implies $p\equiv 1$ or 3 mod 8. Then $x'^2-x'+1$ is a product of primes that are all 1 or 3 mod 8, so $x'^2-x'+1\equiv 1$ or 3 mod 8. But $y'^2\equiv 0,1,$ or 4 mod $8\Rightarrow x'^3=2y'^2+3\equiv$

3 or 5 mod 8 $\Rightarrow x' \equiv 3$ or 5 mod 8. Then $x'^2 - x' + 1 \equiv 1 - x' + 1 \equiv 2 - x' \equiv 5$ or 7 mod 8. That contradicts $x'^2 - x' + 1 \equiv 1$ or 3 mod 8. □

As an exercise, show each of the following has no integral solutions by methods like those used above. In each case, begin by showing x is odd (this is trickier for the third equation).

(1) $y^2 = x^3 - 3$ (Hint: $y^2 + 4 = x^3 + 1$).
(2) $y^2 = x^3 - 9$ (Hint: $y^2 + 1 = x^3 - 8$).
(3) $y^2 = x^3 - 12$ (Hint: $y^2 + 4 = x^3 - 8$).

3. Examples with Solutions

We will now look at some instances of Mordell's equation that have integral solutions. The goal in each case is to find *all* the integral solutions. The main tool we will use is unique factorization (in different settings), and after some successes we will see that this technique eventually runs into difficulties.

We start with the case $k = 16$: the equation $y^2 = x^3 + 16$. There are two obvious integral solutions: $(x, y) = (0, \pm 4)$. A numerical search does not reveal additional integral solutions, so one might guess[3] that $(0, 4)$ and $(0, -4)$ are the only integral solutions. To prove this, we will use unique factorization in $\mathbf{Z}$.

Theorem 3.1. *The only integral solutions to* $y^2 = x^3 + 16$ *are* $(x, y) = (0, \pm 4)$.

Proof. First we determine the parity of an integral solution. Rewrite the equation as $x^3 = y^2 - 16 = (y + 4)(y - 4)$. If y is odd then $(y + 4, y - 4) = 1$ (why?), so both $y + 4$ and $y - 4$ are cubes because their product is a cube. They differ by 8, and no odd cubes differ by 8. Hence y is even, so x is even.

The right side of $y^2 = x^3 + 16$ is divisible by 8, so $4 \mid y$. Writing $y = 4y'$, $16y'^2 = x^3 + 16$. Therefore $4 \mid x$. Write $x = 4x'$, so $y'^2 = 4x'^3 + 1$, showing y' is odd. Write $y' = 2m + 1$, so $4m^2 + 4m + 1 = 4x'^3 + 1$. Thus $m^2 + m = x'^3$. Since $m^2 + m = m(m+1)$ and $(m, m+1) = 1$, the product $m(m + 1)$ being a cube implies (since ± 1 are cubes) both m and $m + 1$ are cubes. The only consecutive cubes are among $\{-1, 0, 1\}$, so m or $m + 1$ is 0. Therefore $x' = 0$, so $x = 0$ and $y = \pm 4$. □

For the next few results, we use unique factorization in $\mathbf{Z}[i]$ or $\mathbf{Z}[\sqrt{-2}]$.

Theorem 3.2. *The only* $x, y \in \mathbf{Z}$ *satisfying* $y^2 = x^3 - 1$ *is* $(x, y) = (1, 0)$.

Proof. First we check the parity of an integral solution. Suppose x is even, so $y^2 + 1 = x^3 \equiv 0$ mod 8. Then $y^2 \equiv -1$ mod 8. But -1 mod 8 is not a square. We have a contradiction, so x is odd, which means y has to be even.

Write the equation $y^2 = x^3 - 1$ as

$$x^3 = y^2 + 1,$$

which in $\mathbf{Z}[i]$ has the factored form

$$x^3 = (y + i)(y - i). \tag{10}$$

If the two factors on the right side are relatively prime in $\mathbf{Z}[i]$, then since their product is a cube, each factor must be a cube up to unit multiple, by unique factorization in $\mathbf{Z}[i]$.

[3] It's a tricky business to decide when to stop searching: $y^2 = x^3 + 24$ has integral solutions at $x = -2, 1, 10$, and 8158 (and no others). Contrast that with $y^2 = x^3 - 24$ in Theorem 2.8. The equation $y^2 = x^3 - 999$ has integral solutions at $x = 10, 12, 40, 147, 174$, and 22480 (and no others) [17].

Moreover, since every unit in $\mathbf{Z}[i]$ is a cube ($1 = 1^3$, $-1 = (-1)^3$, $i = (-i)^3$, $-i = i^3$), unit factors can be absorbed into the cubes. Thus, provided we show $y+i$ and $y-i$ are relatively prime, (10) tells us $y+i$ and $y-i$ are themselves cubes.

To see that $y+i$ and $y-i$ are relatively prime, let δ be a common divisor. Since δ divides $(y+i)-(y-i) = 2i$, $\mathrm{N}(\delta)$ divides $\mathrm{N}(2i) = 4$. Also $\mathrm{N}(\delta)$ divides $\mathrm{N}(y+i) = y^2+1 = x^3$, which is odd. Therefore $\mathrm{N}(\delta)$ divides 4 and is odd, which means $\mathrm{N}(\delta) = 1$, so δ is a unit.

Now that we know $y+i$ and $y-i$ are relatively prime, we must have (as argued already)

$$y + i = (m + ni)^3$$

for some $m, n \in \mathbf{Z}$. Expanding the cube and equating real and imaginary parts,

$$y = m^3 - 3mn^2 = m(m^2 - 3n^2), \quad 1 = 3m^2n - n^3 = n(3m^2 - n^2).$$

The equation on the right tells us $n = \pm 1$. If $n = 1$, then $1 = 3m^2 - 1$, so $3m^2 = 2$, which has no integer solution. If $n = -1$, then $1 = -(3m^2 - 1)$, so $m = 0$. Therefore $y = 0$, so $x^3 = y^2 + 1 = 1$. Thus $x = 1$. □

Theorem 3.3. *The only $x, y \in \mathbf{Z}$ satisfying $y^2 = x^3 - 4$ are $(x, y) = (2, \pm 2)$ and $(5, \pm 11)$.*

Proof. We rewrite $y^2 = x^3 - 4$ in $\mathbf{Z}[i]$ as

$$x^3 = y^2 + 4 = (y + 2i)(y - 2i). \tag{11}$$

We will show that both factors on the right are cubes. Let's first see why this leads to the desired integral solutions. Write

$$y + 2i = (m + ni)^3$$

for some $m, n \in \mathbf{Z}$. Equating real and imaginary parts,

$$y = m(m^2 - 3n^2), \quad 2 = n(3m^2 - n^2).$$

From the second equation, $n = \pm 1$ or $n = \pm 2$. In each case we try to solve for m in $\mathbf{Z}$. The cases that work out are $n = 1$ and $m = \pm 1$, and $n = -2$ and $m = \pm 1$. In the first case, $y = \pm(1 - 3) = \pm 2$ and $x = 2$, while in the second case $y = \pm(1 - 3 \cdot 4) = \pm 11$ and $x = 5$.

It remains to show in (11) that $y + 2i$ and $y - 2i$ are cubes. Since $y^2 \equiv x^3 \bmod 2$ either x and y are both even or they are both odd. We will consider these cases separately, since they affect the greatest common factor of $y + 2i$ and $y - 2i$.

First suppose x and y are both odd. We will show $y + 2i$ and $y - 2i$ are relatively prime in $\mathbf{Z}[i]$. Let δ be a common divisor, so δ divides $(y + 2i) - (y - 2i) = 4i$. Therefore $\mathrm{N}(\delta)$ divides $\mathrm{N}(4i) = 16$. Since $\mathrm{N}(\delta)$ also divides $\mathrm{N}(y + 2i) = y^2 + 4 = x^3$, which is odd, we must have $\mathrm{N}(\delta) = 1$, so δ is a unit. This means $y + 2i$ and $y - 2i$ are relatively prime, so since their product in (11) is a cube and every unit in $\mathbf{Z}[i]$ is a cube, $y + 2i$ and $y - 2i$ are both cubes.

Now suppose x and y are both even. Write $x = 2x'$ and $y = 2y'$, so $4y'^2 = 8x'^3 - 4$. Dividing by 4, $y'^2 = 2x'^3 - 1$. Therefore y' is odd. We must have x' odd too, as otherwise $y'^2 \equiv -1 \bmod 4$, but $-1 \bmod 4$ is not a square. Writing

$$2x'^3 = y'^2 + 1 = (y' + i)(y' - i),$$

the factors on the right each have even norm, so each is divisible by $1 + i$. Divide the equation by $(1 + i)^2 = 2i$:

$$-ix'^3 = \frac{y' + i}{1 + i}\frac{y' - i}{1 + i}.$$

We will show the two factors on the right are relatively prime. Their difference is $2i/(1+i) = 1+i$, so each common divisor has norm dividing $\mathrm{N}(1+i) = 2$. Also each common divisor divides x'^3, so the norm divides $\mathrm{N}(x'^3) = x'^6$, which is odd. Thus each common divisor of $(y'+i)/(1+i)$ and $(y'-i)/(1+i)$ has norm 1, so is a unit. As before, we now know $(y'+i)/(1+i)$ is a cube, so

$$y + 2i = 2(y'+i) = -i(1+i)^2(y'+i) = i^3(1+i)^3\frac{y'+i}{1+i}$$

is a cube in $\mathbf{Z}[i]$. Similarly, $y-2i$ is a cube. □

Theorem 3.4. *The only integral solutions to $y^2 = x^3 - 2$ are $(x,y) = (3, \pm 5)$.*

Proof. Suppose $y^2 = x^3 - 2$ with integral x and y. As in the previous proof, first we do a parity check on x and y. If x is even then $y^2 \equiv -2 \bmod 8$, but $-2 \bmod 8$ is not a square. Therefore x is odd, so y is also odd.

Write the relation between x and y as

$$x^3 = y^2 + 2.$$

In $\mathbf{Z}[\sqrt{-2}]$, we can rewrite this as

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}). \tag{12}$$

The two factors on the right are relatively prime. Indeed, let δ be a common divisor, so δ divides their difference $(y+\sqrt{-2}) - (y-\sqrt{-2}) = 2\sqrt{-2}$, which means $\mathrm{N}(\delta)$ divides $\mathrm{N}(2\sqrt{-2}) = 8$. At the same time, $\mathrm{N}(\delta)$ divides $\mathrm{N}(y+\sqrt{-2}) = y^2+2$, which is odd since y is odd. So $\mathrm{N}(\delta)$ must be 1, which means δ is a unit in $\mathbf{Z}[\sqrt{-2}]$, so $y+\sqrt{-2}$ and $y-\sqrt{-2}$ are relatively prime in $\mathbf{Z}[\sqrt{-2}]$. From (12) and unique factorization in $\mathbf{Z}[\sqrt{-2}]$, $y+\sqrt{-2}$ and $y-\sqrt{-2}$ are both cubes up to unit multiple. The units in $\mathbf{Z}[\sqrt{-2}]$ are ± 1, which are both cubes, and therefore a unit multiple of a cube is also a cube. Hence $y+\sqrt{-2}$ and $y-\sqrt{-2}$ are both cubes.

Write

$$y + \sqrt{-2} = (m + n\sqrt{-2})^3$$

for some $m, n \in \mathbf{Z}$. It follows that

$$y = m^3 - 6mn^2 = m(m^2 - 6n^2), \quad 1 = 3m^2n - 2n^3 = n(3m^2 - 2n^2).$$

From the second equation, $n = \pm 1$. When $n = 1$ the second equation says $1 = 3m^2 - 2$, so $m = \pm 1$. Then $y = \pm 1(1-6) = \pm 5$ and $x^3 = y^2 + 2 = 27$, so we recover the solutions $(x,y) = (3, \pm 5)$. When $n = -1$ we have $1 = -(3m^2 - 2\cdot 1^2) = -(3m^2 - 2)$, so $1 = 3m^2$, which has no solution in $\mathbf{Z}$. □

Remark 3.5. Theorems 3.3 and 3.4 were challenges by Fermat to British mathematicians [4, p. 533], [18, pp. 103, 113]. Fermat said he could solve them by infinite descent, but gave no details. Our proof of Theorems 3.3 and 3.4, like that of Theorem 3.2, studies integers of the form $y^2 + n$ by factoring them in $\mathbf{Z}[\sqrt{-n}]$, which is an idea due to Euler.

Our treatment of $y^2 = x^3 + 16$, $y^2 = x^3 - 1$, $y^2 = x^3 - 4$, and $y^2 = x^3 - 2$ relied on features of $\mathbf{Z}$, $\mathbf{Z}[i]$, and $\mathbf{Z}[\sqrt{-2}]$: they have unique factorization and each unit in them is a cube.

As an exercise, show each of the following three Mordell equations has only the indicated integral solutions by using methods like those above.

(1) $y^2 = x^3 - 8$ in $\mathbf{Z}$ only for $(x,y) = (2,0)$. (Hint: Start by showing y is even.)

(2) $y^2 = x^3 - 16$ has no integral solutions. (Hint: Start by showing y is odd.)
(3) $y^2 = x^3 - 64$ in $\mathbf{Z}$ only for $(x, y) = (4, 0)$. (Hint: Start by showing y is even.)

We can try the same techniques on $y^2 = x^3 + k$ for other values of k. The next three examples illustrate some new features that can occur.

Example 3.6. Consider Mordell's equation with $k = 1$: $y^2 = x^3 + 1$. (Don't confuse this with $y^2 = x^3 - 1$, which is in Theorem 3.2.) There are several obvious integral solutions:

$$(x, y) = (-1, 0), (0, \pm 1), \text{ and } (2, \pm 3).$$

We will use unique factorization in $\mathbf{Z}$ to try to show these are the only integral solutions.[4] This will need a lot more work than our use of unique factorization in $\mathbf{Z}$ to study $y^2 = x^3+16$ in Theorem 3.1.

Rewrite the equation $y^2 = x^3 + 1$ in the form

$$x^3 = y^2 - 1 = (y + 1)(y - 1).$$

The integers $y + 1$ and $y - 1$ differ by 2, so $(y + 1, y - 1)$ is either 1 or 2.

Case 1: y is even. Then $y+1$ and $y-1$ are both odd, so $(y+1, y-1) = 1$. (That is, two consecutive odd integers are always relatively prime.) Since $y+1$ and $y-1$ have a product that is a cube and they are relatively prime, unique factorization in $\mathbf{Z}$ tells us that they are both cubes or both the negatives of cubes. The negative of a cube is also a cube (since $-1 = (-1)^3$), so $y + 1$ and $y - 1$ are both cubes:

$$y + 1 = a^3, \quad y - 1 = b^3.$$

Subtracting, we have $a^3 - b^3 = 2$. Considering how cubes spread apart, the only cubes that differ by 2 are 1 and -1. So $a^3 = 1$ and $b^3 = -1$, meaning $a = 1$ and $b = -1$. Therefore $y + 1 = 1$, so $y = 0$ and $x = -1$. The integral solution $(-1, 0)$ of $y^2 = x^3 + 1$ is the only one where y is even.

Case 2: y is odd, so x is even. We expect to show that the only such integral solutions are $(0, \pm 1)$ and $(2, \pm 3)$. Since $y+1$ and $y-1$ are both even and differ by 2, $(y+1, y-1) = 2$. Either $y \equiv 1 \bmod 4$ or $y \equiv 3 \bmod 4$. Since (x, y) is a solution if and only if $(x, -y)$ is a solution, by negating y if necessary we may assume $y \equiv 1 \bmod 4$. Then $y + 1 \equiv 2 \bmod 4$ and $y - 1 \equiv 0 \bmod 4$. Dividing the equation $x^3 = y^2 - 1$ by 8, we have

$$\left(\frac{x}{2}\right)^3 = \frac{y+1}{2} \cdot \frac{y-1}{4}.$$

The two factors on the right are relatively prime, since $y+1$ and $y-1$ have greatest common factor 2 and we have divided each of them by a multiple of 2. Since the product of $(y-1)/2$ and $(y + 1)/4$ is a cube and the factors are relatively prime, each of them is a cube:

$$\frac{y+1}{2} = a^3, \quad \frac{y-1}{4} = b^3$$

with integers a and b. (Actually, at first we can say $(y + 1)/2$ and $(y - 1)/4$ are cubes up to sign, but $-1 = (-1)^3$ so, as before, we can absorb a sign into a and b if signs occur.) Solving each equation for y,

$$2a^3 - 1 = y = 4b^3 + 1, \tag{13}$$

[4]In fact, these are the only *rational* solutions of $y^2 = x^3 + 1$. That is due to Euler [5, Theorem 10]. A proof by descent is at https://kconrad.math.uconn.edu/blurbs/ugradnumthy/descentbyeuler.pdf.

so $a^3-2b^3=1$. We can spot right away two integral solutions to $a^3-2b^3=1$: $(a,b)=(1,0)$ and $(a,b)=(-1,-1)$. In the first case, using (13) we get $y=1$ (so $x=0$) and in the second case we get $y=-3$ (so $x=2$). We have found two integral solutions to $y^2=x^3+1$ when $y\equiv 1 \bmod 4$: $(0,1)$ and $(2,-3)$. Negating y produces the two solutions $(0,-1)$ and $(2,3)$ where $y\equiv 3 \bmod 4$.

Therefore if $a^3-2b^3=1$ has no integral solution (a,b) besides $(1,0)$ and $(-1,-1)$, the equation $y^2=x^3+1$ has no integral solutions besides the five we know.[5] That the only integral solutions of $a^3-2b^3=1$ are $(1,0)$ and $(-1,-1)$ is a special case of the following general theorem of Delaunay and Nagell [3, pp. 223–226], [7, Sect. VII.3], [9, Sect. 3-9]: *for each nonzero integer d, the equation $a^3-db^3=1$ has at most one integral solution (a,b) with $b\neq 0$*. The cases $d>0$ and $d<0$ are equivalent since the exponent is odd: $a^3-db^3=a^3+d(-b)^3$. Proving the Delaunay–Nagell theorem, even for the special case $d=2$, introduces many new complications (a proof of this special case, using p-adic analysis, is in [15, pp. 34–35][6] or see https://kconrad.math.uconn.edu/blurbs/gradnumthy/x3-2y3=1.pdf), so we omit a proof and refer the reader to the indicated references.

Example 3.7. Consider $y^2=x^3-5$. We have already seen in Theorem 2.2 that this equation has no integral solutions by a method that only uses calculations in $\mathbf{Z}$. Let's try to show there are no integral solutions using factorizations in $\mathbf{Z}[\sqrt{-5}]$.

Start with a parity check. If x is even then $y^2\equiv -5\equiv 3 \bmod 8$, but 3 mod 8 is not a square. Therefore x is odd, so y is even.

Write the equation as

$$x^3=y^2+5=(y+\sqrt{-5})(y-\sqrt{-5}).$$

Suppose δ is a common factor of $y+\sqrt{-5}$ and $y-\sqrt{-5}$. First of all, $\mathrm{N}(\delta)$ divides y^2+5, which is odd. Second of all, since δ divides $(y+\sqrt{-5})-(y-\sqrt{-5})=2\sqrt{-5}$, $\mathrm{N}(\delta)$ divides $\mathrm{N}(2\sqrt{-5})=20$. Therefore $\mathrm{N}(\delta)$ is 1 or 5. If $\mathrm{N}(\delta)=5$ then $5\mid(y^2+5)$, so $5\mid y$. Then $x^3=y^2+5\equiv 0 \bmod 5$, so $x\equiv 0 \bmod 5$. Now x and y are both multiples of 5, so $5=x^3-y^2$ is a multiple of 25, a contradiction. Hence $\mathrm{N}(\delta)=1$, so δ is a unit. This shows $y+\sqrt{-5}$ and $y-\sqrt{-5}$ have no common factor in $\mathbf{Z}[\sqrt{-5}]$ except for units.

Since $y+\sqrt{-5}$ and $y-\sqrt{-5}$ are relatively prime and their product is a cube, they are both cubes (the units in $\mathbf{Z}[\sqrt{-5}]$ are ± 1, which are both cubes). Thus

$$y+\sqrt{-5}=(m+n\sqrt{-5})^3$$

for some integers m and n, so

$$y=m^3-15mn^2=m(m^2-15n^2),\quad 1=3m^2n-5n^3=n(3m^2-5n^2).$$

From the second equation, $n=\pm 1$. If $n=1$ then $1=3m^2-5$, so $3m^2=6$, which has no integral solution. If $n=-1$ then $1=-(3m^2-5)$, so $3m^2=4$, which also has no integral solution. We appear to have recovered the fact that $y^2=x^3-5$ has no integral solutions.

Alas, there is an error in Example 3.7. When we wrote certain numbers in $\mathbf{Z}[\sqrt{-5}]$ as cubes, we were implicitly appealing to unique factorization in $\mathbf{Z}[\sqrt{-5}]$, which is in fact false.

[5]The converse is true too: every integral solution of $a^3-2b^3=1$ leads to the integral solution $(x,y)=(2ab,4b^3+1)$ of $y^2=x^3+1$, so if $y^2=x^3+1$ only has the five integral solutions we know then from $a^3-2b^3=1$ we must have $(2ab,4b^3+1)=(0,1)$ or $(2,-3)$ since these are the only (x,y) with $y\equiv 1 \bmod 4$, and from this it easily follows that $(a,b)=(1,0)$ and $(-1,-1)$.

[6]In fact, $(1,0)$ and $(-1,-1)$ are the only *rational* solutions of $x^3-2y^3=1$, a result first due to Euler [6, Part II, Sect. II, § 247].

A counterexample to unique factorization in $\mathbf{Z}[\sqrt{-5}]$ is $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. That doesn't mean the numbers in $\mathbf{Z}[\sqrt{-5}]$ that we wanted to be cubes might not be cubes, but our justification for those conclusions is certainly faulty. It *is* true in $\mathbf{Z}[\sqrt{-5}]$ that if $\alpha\beta$ is a cube and α and β are relatively prime then α and β are both cubes, but to explain why requires new techniques to circumvent the lack of unique factorization.

Example 3.8. Consider $y^2 = x^3 - 26$. Two obvious integral solutions are $(3, \pm 1)$. Let's use factorizations in $\mathbf{Z}[\sqrt{-26}]$ to see if $(3, \pm 1)$ are the only integral solutions.

If x is even then $y^2 \equiv -26 \equiv 6 \bmod 8$, but 6 mod 8 is not a square. Therefore x is odd, so y is odd too. Rewrite $x^3 = y^2 + 26$ as $x^3 = (y + \sqrt{-26})(y - \sqrt{-26})$. Let δ be a common factor of $y+\sqrt{-26}$ and $y-\sqrt{-26}$ in $\mathbf{Z}[\sqrt{-26}]$. Then $\mathrm{N}(\delta)$ divides y^2+26, which is odd. Also δ divides the difference $(y + \sqrt{-26}) - (y - \sqrt{-26}) = 2\sqrt{-26}$, so $\mathrm{N}(\delta)$ divides $4 \cdot 26 = 8 \cdot 13$. Since $\mathrm{N}(\delta)$ is odd, we see that $\mathrm{N}(\delta)$ is 1 or 13. There is no element of $\mathbf{Z}[\sqrt{-26}]$ with norm 13, so $\mathrm{N}(\delta) = 1$. Therefore $\delta = \pm 1$, so $y + \sqrt{-26}$ and $y - \sqrt{-26}$ have only ± 1 as common factors.

If we assume $\mathbf{Z}[\sqrt{-26}]$ has unique factorization, then since $y + \sqrt{-26}$ and $y - \sqrt{-26}$ multiply to a cube and they have only ± 1 as common factors, each of them is a cube. Write

$$y + \sqrt{-26} = (m + n\sqrt{-26})^3,$$

so

$$y = m^3 - 78mn^2 = m(m^2 - 78n^2), \quad 1 = 3m^2n - 26n^3 = n(3m^2 - 26n^2).$$

The second equation tells us $n = \pm 1$. If $n = 1$ then $1 = 3m^2 - 26$, so $3m^2 = 27$, which tells us $m = \pm 3$. Then $y = (\pm 3)(9 - 78) = \pm 207$ and $x^3 = 207^2 + 26 = 42875 = 35^3$, so $x = 35$. We have discovered new integral solutions to $y^2 = x^3 - 26$, namely $(x, y) = (35, \pm 207)$. If $n = -1$ then $1 = -(3m^2 - 26)$, so $3m^2 = 25$, which has no integral solutions.

Having looked at both possible values of n, we discovered two unexpected integral solutions, but we *missed* the obvious integral solutions $(3, \pm 1)$! How could that happen? The reason is that our argument was based on the assumption of unique factorization in $\mathbf{Z}[\sqrt{-26}]$, but there is not unique factorization in $\mathbf{Z}[\sqrt{-26}]$. A counterexample is

$$27 = 3 \cdot 3 \cdot 3 = (1 + \sqrt{-26})(1 - \sqrt{-26}).$$

It is true that the only integral solutions to $y^2 = x^3 - 26$ are $(3, \pm 1)$ and $(35, \pm 207)$, but a valid proof has to get around the lack of unique factorization in $\mathbf{Z}[\sqrt{-26}]$.

4. Rational solutions

For $k \in \mathbf{Z}$, if we consider rational solutions to $y^2 = x^3 + k$ instead of integral solutions, the situation gets much more complicated. First of all, there could be rational solutions even if there are no integral solutions. For instance, $y^2 = x^3 + 11$ has no integral solutions by Theorem 2.3, but this equation has the rational solution $(x, y) = (-7/4, 19/8)$. In fact, $y^2 = x^3+11$ has infinitely many rational solutions. Second of all, sometimes the only rational solutions are the integral solutions, but proving that is much harder than determining all the integral solutions.

To emphasize the distinction between classifying integral and rational solutions, consider $y^2 = x^3+16$. We proved the only integral solutions are $(0, \pm 4)$ in Theorem 3.1. This does not tell us whether there are rational solutions of $y^2 = x^3+16$ that are not integral. It turns out there are no further rational solutions, and here is an application of that. If $a^3+b^3 = c^3$ for nonzero integers a, b, and c, then the nonzero rational numbers $(x, y) = (4bc/a^2, 4+8(b/a)^3)$ satisfy $y^2 = x^3 + 16$. (I found this choice in [2], and moving terms around in the equation

$a^3 + b^3 = c^3$ leads to other rational solutions of $y^2 = x^3 + 16$. What do you get from $c^3 + (-b)^3 = a^3$?) Proving the only rational solutions to $y^2 = x^3 + 16$ are $(0, \pm 4)$ would force $x = 0$, but $x = 4bc/a^2 \neq 0$, so knowing the only *rational* solutions of $y^2 = x^3 + 16$ are $(0, \pm 4)$ implies Fermat's Last Theorem for exponent 3.

The following table describes all the integral solutions for the cases of Mordell's equation we have looked at. (The examples $k = 1$ and -26 were not fully justified above.)

k	**Z**-solutions of $y^2 = x^3 + k$
1	$(-1, 0), (0, \pm 1), (2, \pm 3)$
-1	$(1, 0)$
-2	$(3, \pm 5)$
-4	$(2, \pm 2), (5, \pm 11)$
-5	None
6	None
-6	None
7	None
11	None
16	$(0, 4), (0, -4)$
-24	None
-26	$(3, \pm 1), (35, \pm 207)$
45	None
46	None

In each case there are finitely many integral solutions, and $y^2 = x^3 + k$ has finitely many integral solutions for every nonzero k in **Z**. If we look at rational solutions, then we might not get anything new, but we could get a lot that is new. See the next table.

k	**Q**-solutions of $y^2 = x^3 + k$
1	$(-1, 0), (0, \pm 1), (2, \pm 3)$
-1	$(1, 0)$
-2	Infinitely many
-4	Infinitely many
-5	None
6	None
-6	None
7	None
11	Infinitely many
16	$(0, 4), (0, -4)$
-24	None
-26	Infinitely many
45	None
46	Infinitely many

The equations above that have more rational solutions than integral solutions are $y^2 = x^3 - 2$, $y^2 = x^3 - 4$, $y^2 = x^3 + 11$, $y^2 = x^3 - 26$, and $y^2 = x^3 + 46$. Examples of rational solutions to these equations that are not integral solutions are in the following table.

k	-2	-4	11	-26	46
Q-soln	$\left(\frac{129}{100}, \frac{383}{1000}\right)$	$\left(\frac{106}{9}, \frac{1090}{27}\right)$	$\left(-\frac{7}{4}, \frac{19}{8}\right)$	$\left(\frac{705}{4}, \frac{18719}{8}\right)$	$\left(-\frac{7}{4}, \frac{51}{8}\right)$

References

[1] S. Alaca and K. S. Williams, "Introductory Algebraic Number Theory," Cambridge Univ. Press, Cambridge, 2004.

[2] T. R. Bendz, Öfver diophantiska ekvationen $x^n + y^n = z^n$, Ph.D. thesis, Uppsala Univ., 1901.

[3] J. W. S. Cassels, "Local Fields," Cambridge Univ. Press, Cambridge, 1986.

[4] L. E. Dickson, "History of the Theory of Numbers," Vol. II, Chelsea, Bronx, 1971.

[5] L. Euler, *Theorematum quorundam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petrop. **10** (1738), 125–146. English translation URL https://scholarlycommons.pacific.edu/euler-works/98/.

[6] L. Euler, "Elements of Algebra," 1770. English translation URL http://www.17centurymaths.com/contents/euleralgebra.htm.

[7] A. Fröhlich, M. J. Taylor, "Algebraic Number Theory," Cambridge Univ. Press, Cambridge, 1993.

[8] V. A. Lebesgue, *Notes sur quelques équations indéterminées*, Nouvelles Annales de Mathématiques, 2e sér., **8** (1869), 452–456.

[9] W. J. Leveque, "Topics in Number Theory, Volume II," Addison-Wesley, Reading, MA, 1956.

[10] L. J. Mordell, *A Statement by Fermat*, Proceedings of the London Math. Soc. **18** (1920), v-vi.

[11] L. J. Mordell, "A Chapter in the Theory of Numbers," Cambridge Univ. Press, 1947.

[12] L. J. Mordell, "Two Papers on Number Theory," VEB Deutscher Verlag der Wissenschaften, Berlin, 1972.

[13] H. N. Shapiro, "Introduction to the Theory of Numbers," Wiley, New York, 1983.

[14] H. N. Shapiro and G. H. Sparer, "Power-quadratic Diophantine Equations and Descent," *Comm. Pure and Applied Math.* **31** (1978), 185–203. (Corrections in **32** (1979), 277–279.)

[15] N. P. Smart, "The Algorithmic Resolution of Diophantine Equations," Cambridge Univ. Press, Cambridge, 1998.

[16] H. M. Stark, "An Introduction to Number Theory," MIT Press, Cambridge, 1978.

[17] R. P. Steiner, *On Mordell's Equation $y^2 - k = x^3$: A Problem of Stolarsky*, Math. Comp. **47** (1986), 703–714.

[18] A. Weil, "Number Theory: An Approach Through History; from Hammurapi to Legendre," Birkhäuser, Boston, 1984.